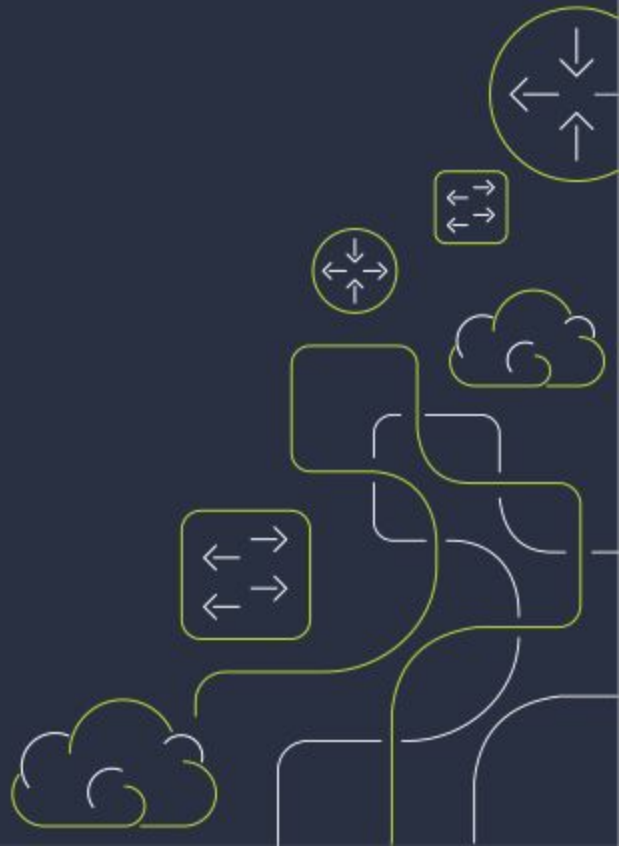
Ataques DDoS:
o que fazer antes do primeiro ataque?

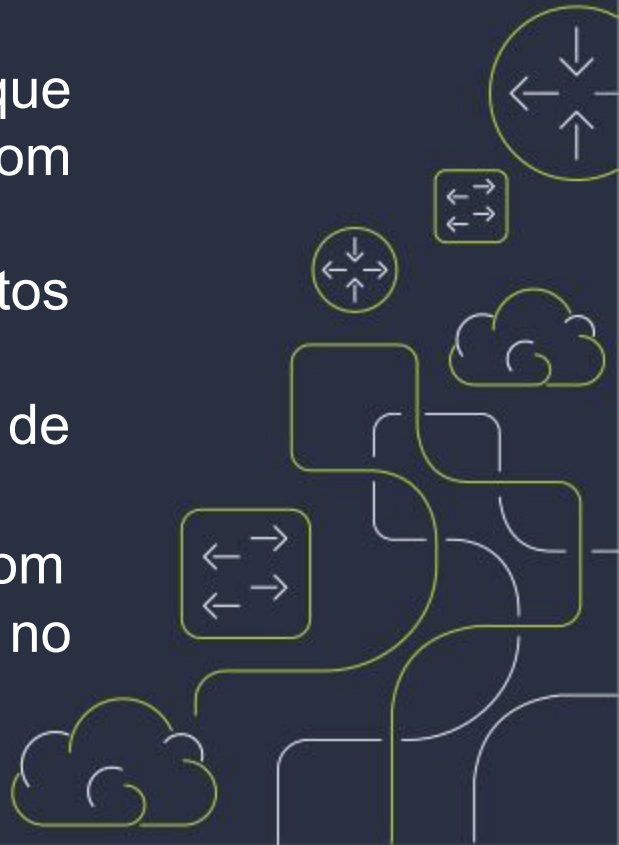
por T. Ayub
Diretor de Tecnologia

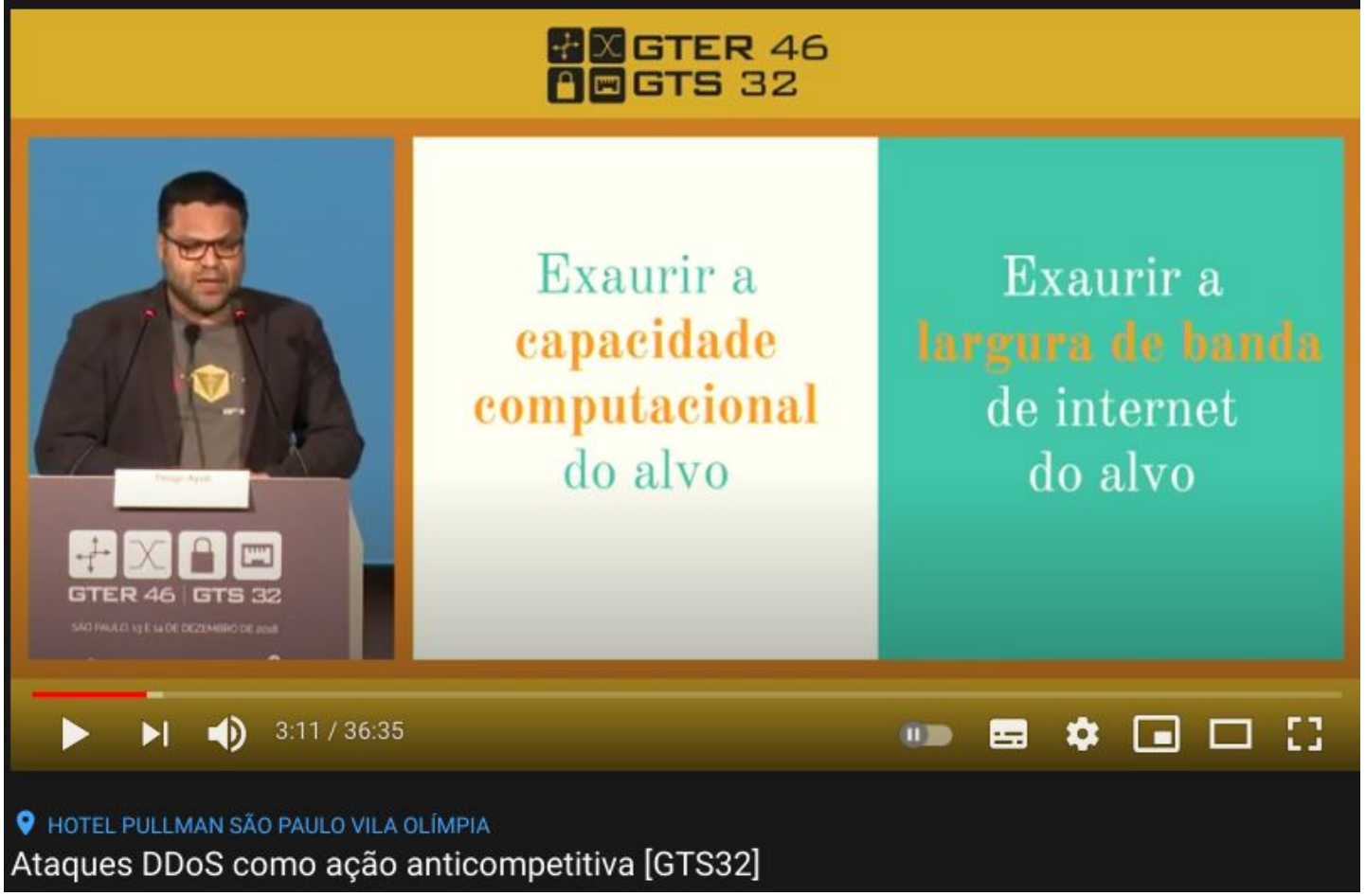


E o que são ataques DDoS?

São ataques a redes dos ISPs e data centers que tem como objetivo deixá-las fora do ar ou com performance severamente degradada.

- Saturam toda a **banda** disponível com trânsitos IP e IX.
- Saturam a capacidade computacional **(CPU)** de roteadores, concentradores PPPoE e CGNAT.
- Exaurem o **recurso humano** de seu ISP, com jornadas longas de trabalho, filas elevadas no *call center*.

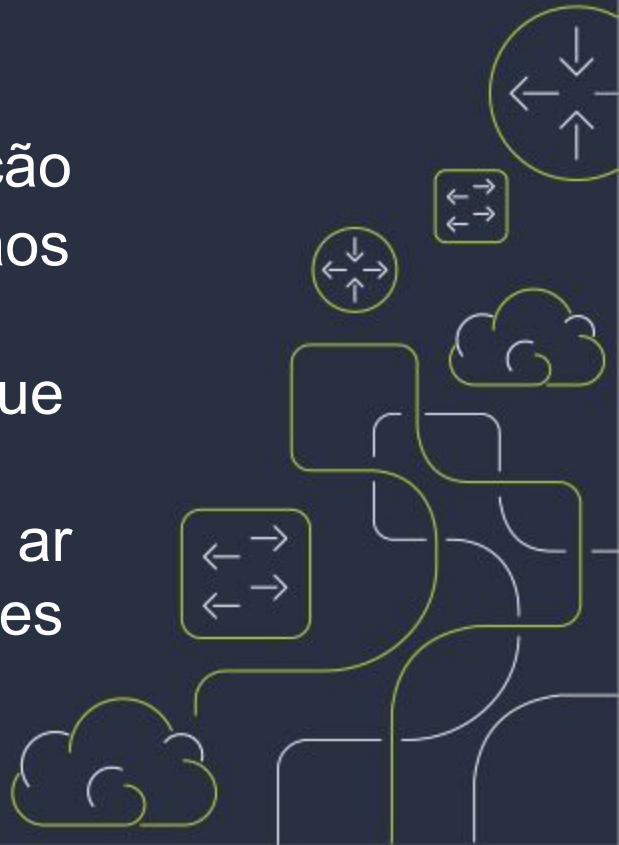




youtube.com/c/ayubio

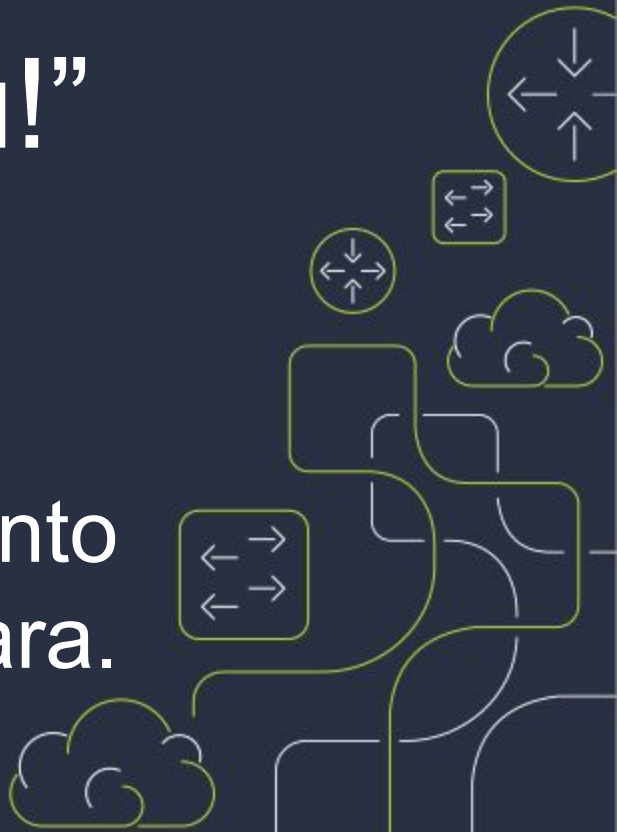
Então quem procura a Sage?

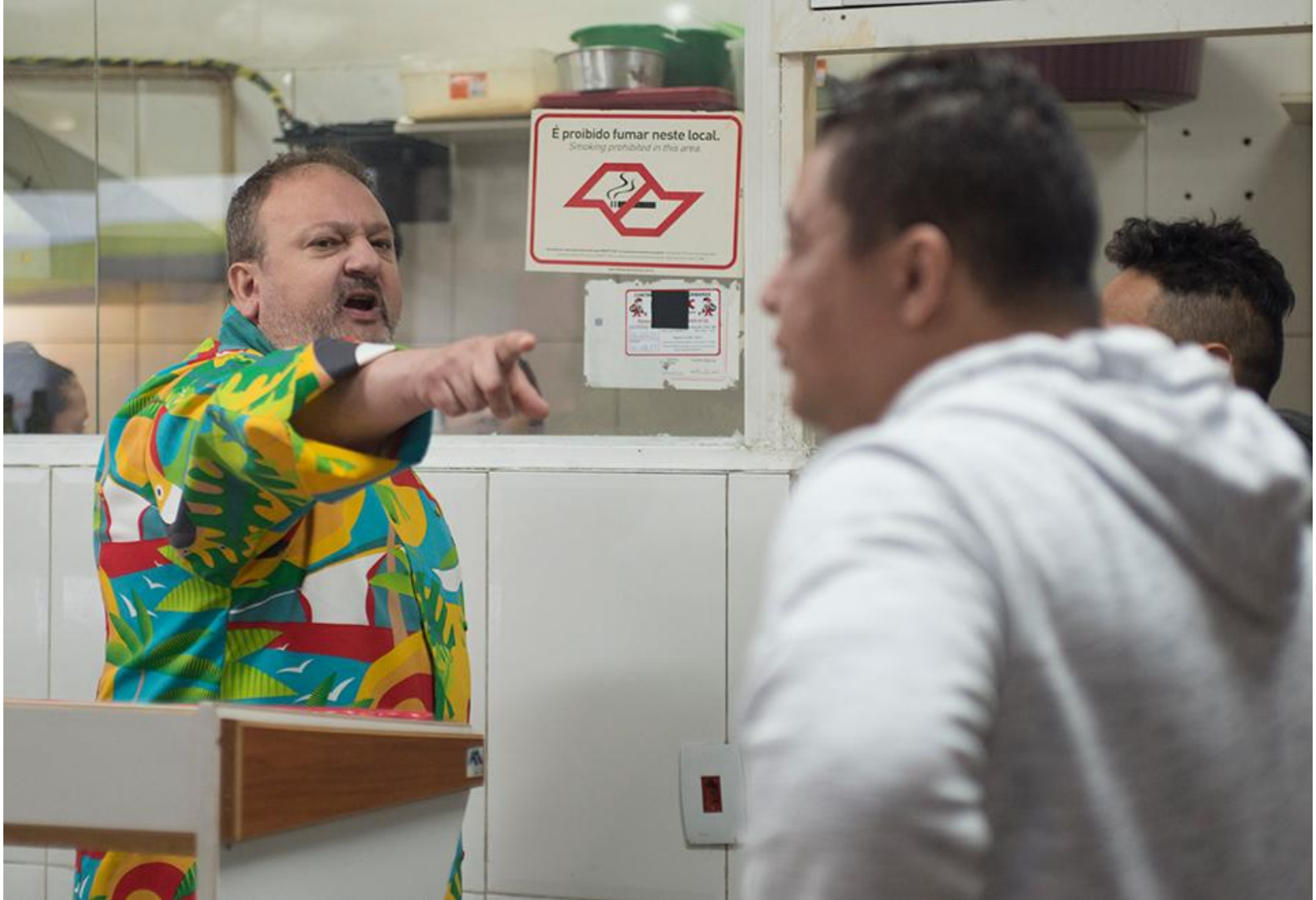
- Quem quer montar um centro de mitigação na sua rede para **vender** esse serviço aos seus clientes.
- Quem quer **evitar** que seu negócio fique fora do ar por conta desse tipo de ataque.
- Quem já está totalmente fora do ar **totalmente fora do ar** por conta desses ataques.



- “A cavalaria chegou!”
- “Os bombeiros chegaram!”

… mas na verdade me sinto um outro cara.

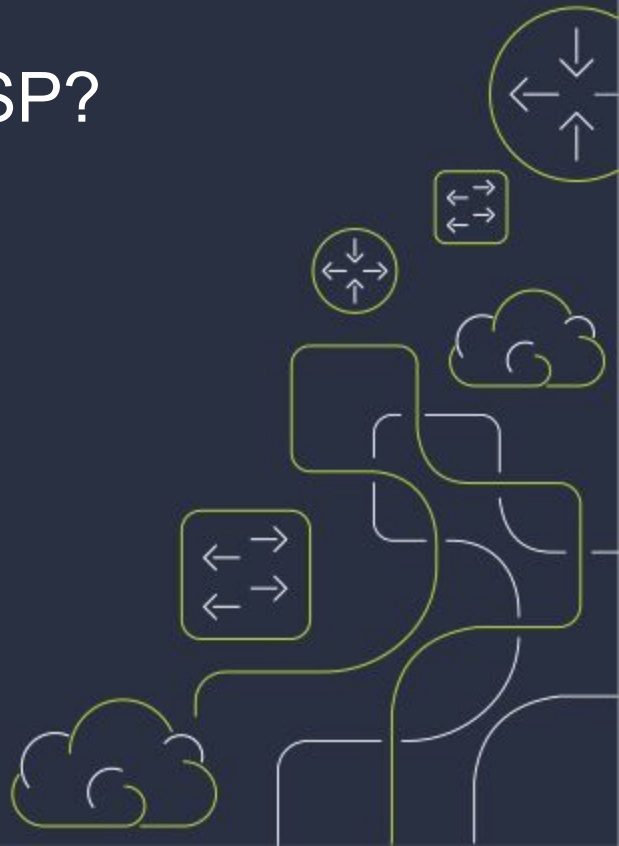



É proibido fumar neste local.
Smoking prohibited in this area.

Quais são os 3 modos?

Quais são os 3 modos de se fazer um ISP?

- O modo **errado**.
- O modo **certo**.
-

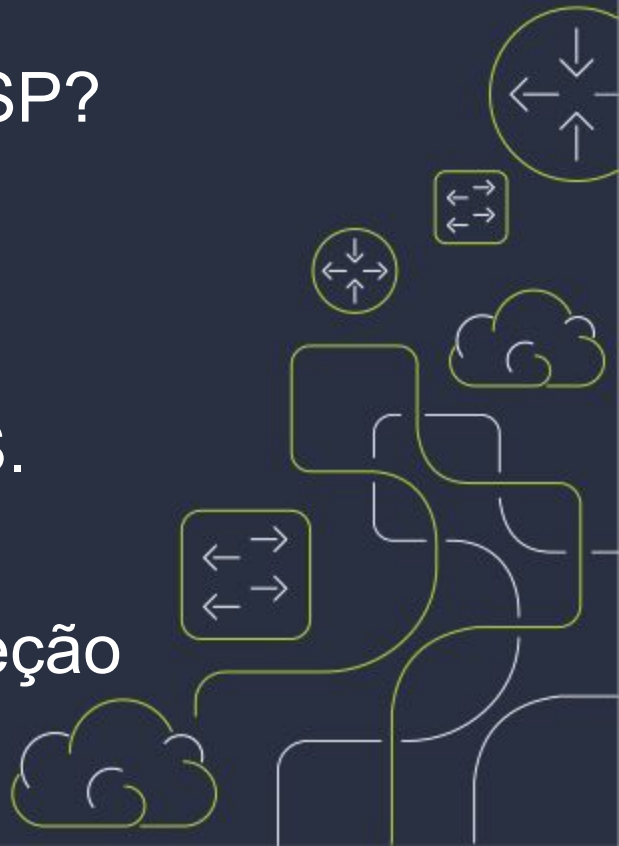


Quais são os 3 modos?

Quais são os 3 modos de se fazer um ISP?

- O modo **errado**.
- O modo **certo**.
- O modo **resistente** a ataques DDoS.

O DDoS cobra à vista, com juros e correção monetária o débito **técnico** da sua rede.



Sobre o ataque em si

O que você precisa saber:

- O atacante **não** será **identificado**.
- Sua operadora **não** vai **resolver** o problema.
- A temporada de ataque costuma durar **meses**.
- O ataque é fácil e **barato** de ser feito.
- Se você nunca foi atacado, com o passar do tempo o **risco** aumenta.

Bronze Monthly

$ 10 .00

1 Concurrent
300 seconds boot time
700Gbps total booter network capacity
Dedicated Support
Access to DDOS tools

Sign Up

Gold Monthly

$ 35 .00

1 Concurrent
1200 seconds boot time
700Gbps total booter network capacity
Dedicated Support
Access to DDOS tools

Sign Up

Platinum Monthly

$ 50 .00

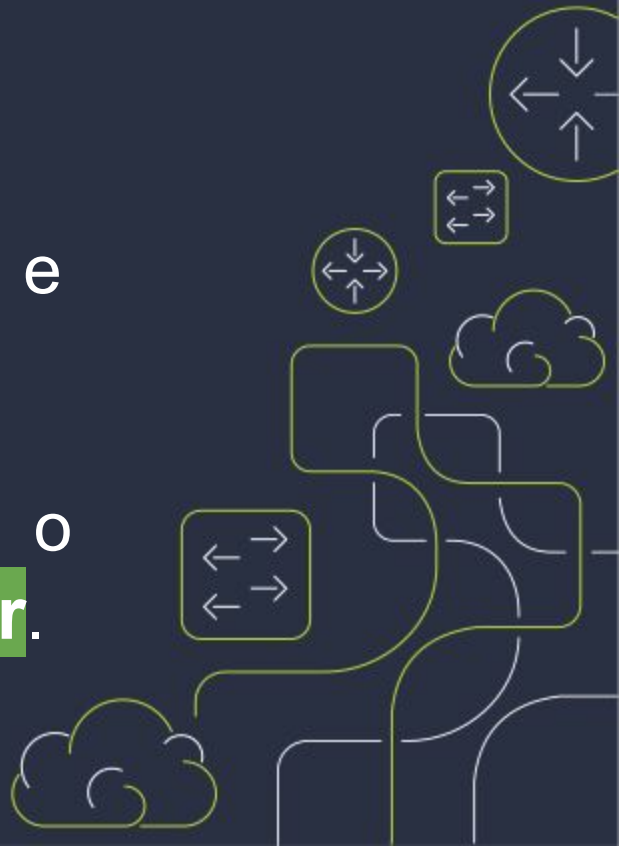
1 Concurrent
2500 seconds boot time
700Gbps total booter network capacity
Dedicated Support
Access to DDOS tools

Sign Up

Sobre a mitigação

O que você precisa saber:

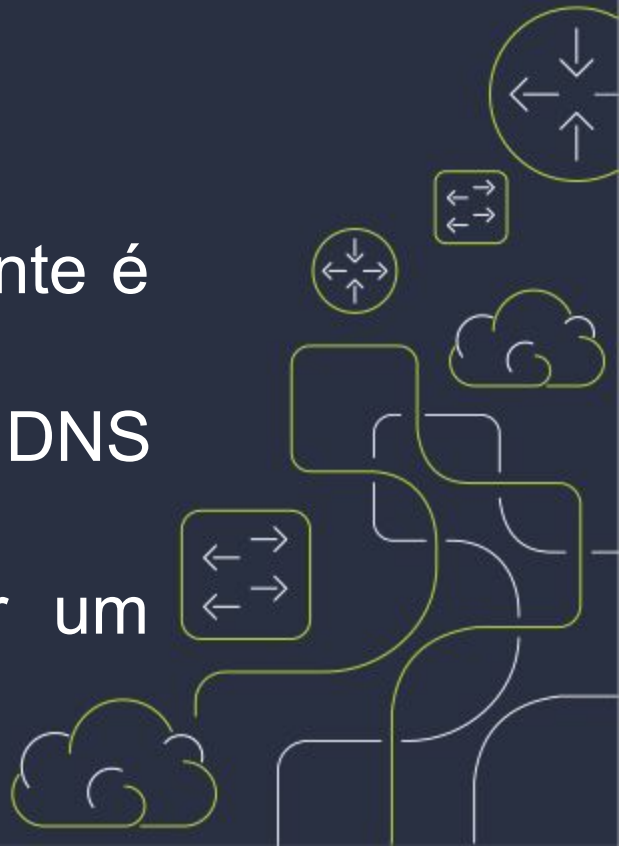
- A implantação dela dura dias **dias** e não horas.
- Ela vai gerar **efeitos colaterais**.
- Se sua rede não estiver sólida o suficiente você continuará **fora do ar**.



O que você precisa fazer?

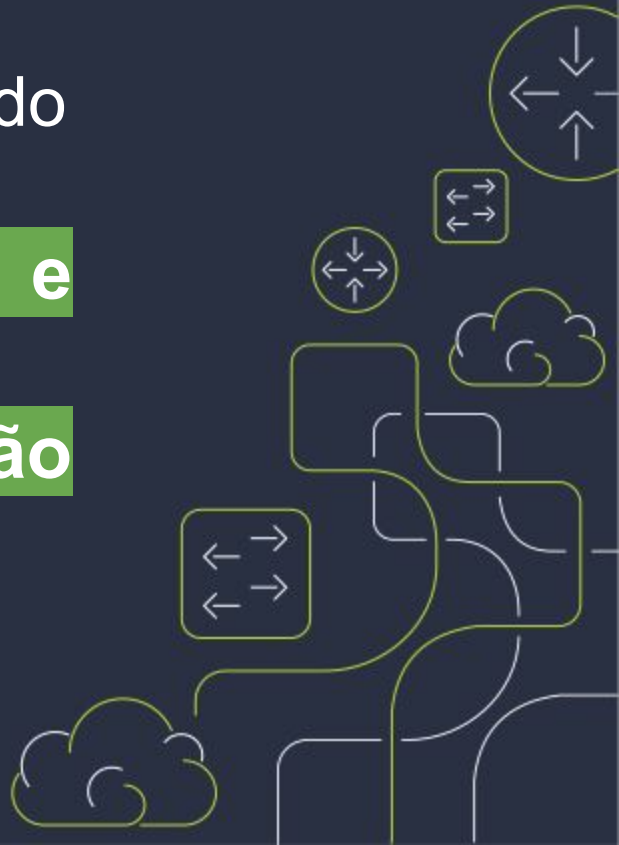
Antes do primeiro ataque:

- Por o **IPv6** em produção. Parcialmente é melhor que nada.
- Rodar seus servidores de DNS **localmente**.
- Trocar seu roteador de borda por um ***hardware based***.



O que você precisa fazer?

- Separe seu time de **engenharia** do time do suporte.
- Implante um sistema de **detecção e automação** de resposta a ataques.
- Contrate uma **nuvem de mitigação** antes do primeiro ataque.



Dúvidas?

E-mail: thiago.ayub@sagenetworks.com.br
Instagram: @AyubioNET / @sage_networks

Site: sagenetworks.com.br
Telefone: (19) 3500-6269